UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/676,474 | 09/30/2003 | Klimenty Vainstein | 2222.5450000 | 7534 |

26111 7590 02/24/2011

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

| EXAMINER | |
|---|---|
| ZEE, EDWARD | |
| **ART UNIT** | **PAPER NUMBER** |
| 2435 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/24/2011 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/676,474 | VAINSTEIN ET AL. | |
| | Examiner | Art Unit | |
| | EDWARD ZEE | 2435 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,13-18 and 21-28* is/are rejected.

7)☒ Claim(s) *12,19 and 20* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This is in response to the correspondence filed on 07/13/10. Claims 1, 5, 14, 21, 22, 27 and 28 have been amended; Claims 1-28 are pending and have been considered below.

## Docketing

Please note that the application has been docketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final sections of the office action.

## Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **07/13/10** has been entered.

## Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

**Claims 27 and 28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** The instant claims are directed to a "computer readable storage medium", which in light of the disclosure (please see page 24 of the

specification), does not appear to explicitly exclude transitory media and thus would be reasonably interpreted to encompass electronic signals. A signal is not a series of steps or acts and this is not a process. A signal is not a physical article or object and as such is not a machine or manufacture. A signal is not a combination of substances and therefore not a compilation of matter. Thus, a signal by itself does not fall within any of the four categories of invention. Therefore, Claims 27 and 28 are not statutory.

## Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**5. Claims 1-8, 11, 13-18, 21 and 23-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis et al. (6,584,466) in view of Troyansky et al. (2005/0168766, submitted in the IDS dated 11/16/10).**

**Claim 1:** Serbinis discloses a document security system for restricting access to secured documents (See Fig. 1-5) comprising:

a processor (see, Fig. 1B, numerals 20 A, 20 B);

a policy module configured to enable the processor to store at least one process-driven security policy (see, Column 7, lines 63-67, "document state process") on a computer readable storage medium, wherein the process-driven security policy includes a plurality of different states (see, Column 7 line 67- Column 8, line 4, "pending," and "active," states. Note: examiner

is equating only pending and active to the claimed plurality of different states) and transition rules (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.""), wherein each of the different states is associated with one or more access restrictions, and wherein each of the different states has distinct access restrictions for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.") and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.") and wherein the circumstances include the occurrence of internal and external events (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation).

an access manager module configured to enable the processor to access the process-driven security policy and determine whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy (see,

Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20, Column 9, line 64- Column 10 line 5 describing the authentication process and Column 8, lines 1-20, discloses a "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users, so the authentication step determine the access based on policy state associated therewith at the time access is requested and the corresponding one or more access restriction thereof for the process-driven security policy).

However, Serbinis does not explicitly discloses wherein the external events originate from outside the policy system; nor wherein the policy system is configured to enable the processor to provide a reference to the process-driven security policy to a client computer, the referencing referring to the process-driven security policy and an accessor user list resident on the policy system.

Nonetheless, Troyansky et al. discloses a similar invention and further discloses wherein the external events originate from outside the policy system(central decision system) [page 19, paragraph 0899]; and wherein the policy system is configured to enable the processor to provide a reference(marking module is instructed to embed a marking indicating at least the existence of policy) [page 22, paragraph 0945] to the process-driven security policy to a client computer, the referencing referring to the process-driven security policy and an accessor user list resident on the policy system*(allowed recipients information for an associated document...certain group of* individuals can override a specified subset of the security provisions for a group of documents) [page 3, paragraph 0119 & page 19, paragraph 0897].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Serbinis with the additional features of Troyansky

et al., in order to allow for monitoring and controlling of unauthorized dissemination of electronic documents on a portable media and enforcement of a distribution policy associated with the documents, as suggested by Troyansky et al. [page 1, paragraphs 0005-0007].

Regarding **Claim 2**, the rejection of claim 1 is incorporated and Serbinis further discloses that the one or more access restrictions for the secured document are automatically changed in response to detecting a change in the state of the process-driven security policy for the secured document (see Column 7, lines 63-67).

Regarding **Claim 3**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another (see, Column 7, lines 63-67).

Regarding **Claim 4**, the rejection of claim 3 is incorporated and Serbinis further discloses wherein the internal events originate from the document security system and wherein external events originate from outside the document security system (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time").

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Serbinis further discloses that at least one of the events is an external event from a document management system (see Column 8, lines 26-30).

Regarding **Claim 6**, the rejection of claim 1 is incorporated and Serbinis further discloses that one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes (see paragraph 0123)

Regarding **Claim 7**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see Column 7, lines 63-67).

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state and a third state and second event that causes transition from the second state to a third state (see, Column 8, lines 1-20).

Regarding **Claim 8**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see Column 7, lines 63-67).

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state (see Column 8, lines 1-20).

Regarding **Claim 11**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state, and wherein the secured document is modified in response to detecting a transition from the previous state of the process-driven security policy for the secured document (see Column 7, lines 63-67).

Regarding **Claim 13**, the rejection of claim 11 is incorporated and Serbinis further discloses wherein in response to determining, by the access manager, that access to a secured document is permitted by a requestor, access to the secured document is available at a client machine associated with the requestor (see, Column 9 line 66- Column 10, line 5, "The Authorized User may then request retrieval of the document from store 30, at step 88, and any automatic filtering, or filtering selected by the Authorized User, may be performed during the document download process at step 89. The document is then downloaded to the Authorized User at step 90. Each transaction is logged to the appropriate tables of DMS database 25.").

**Claims 14 and 27:** Serbinis discloses a method and a corresponding software program for transitioning at least one secured document through a security-policy state machine having a plurality of different states (see, Column 7 line 67- Column 8, line 4, "pending," and "active," states, Note: examiner is equating only pending and active states to the claimed plurality of different states), each of the plurality of different states having distinct access restrictions for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users."), the method comprising:

receiving an event (see, Column 7, lines 63-67, "the active date/time, and expiration date/time"), wherein the event is one of a group on internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator)

forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation).

determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent different state of the security-policy state machine; (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process")

automatically transitioning from the former state to the subsequent different state of the security-policy state machine in response to determining that the event causes the state transition (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time.")

However, Serbinis does not explicitly disclose wherein the external events originate from outside the security-policy state machine; nor providing a reference to the security-policy state machine to a client computer, the reference referring to a current state of the security-policy state machine and an accessor user list resident in the security-policy state machine.

Nonetheless, Troyansky et al. discloses a similar invention and further discloses wherein the external events originate from outside the security-policy state machine(central decision system) [page 19, paragraph 0899]; and providing a reference to the security-policy state machine to a client computer, the reference referring to a current state of the security-policy state machine and an accessor user list resident in the security-policy state machine(allowed recipients *information for an associated document...certain group of individuals can override a specified*

subset of the security provisions for a group of documents) [page 3, paragraph 0119 & page 19, paragraph 0897].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Serbinis with the additional features of Troyansky et al., in order to allow for monitoring and controlling of unauthorized dissemination of electronic documents on a portable media and enforcement of a distribution policy associated with the documents, as suggested by Troyansky et al. [page 1, paragraphs 0005-0007].

Regarding **Claim 15**, the rejection of claim 14 is incorporated and Serbinis further discloses the security-policy state machine implements a process-driven security policy, and wherein each state of the security-policy state machine has different access restrictions (see Column 8, lines 1-20).

Regarding **Claim 16**, the rejection of claim 14 is incorporated and Serbinis further discloses each of the states of the security-policy state machine have different access policies (see Column 8, lines 1-20).

Regarding **Claim 17**, the rejection of claim 16 is incorporated and Serbinis further discloses the security-policy state machine is provided as part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system (See, Column 8, lines 1-20 and Column 9, line 63- Column 10, line 5)

Regarding **Claim 18**, the rejection of claim 14 is incorporated and Serbinis further discloses wherein the transitioning comprises modifying the secured document to reflect the subsequent state of the security-policy state machine (see Column 7, lines 63-67).

**Claim 21:** Serbinis discloses a method and corresponding computer program for imposing access restrictions on electronic documents, the method comprising:

providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of different states (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and wherein each of the different states has distinct access restriction for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.");

transitioning the process-driven security policy from one state to a current state (see, Column 8, lines 1-20) in response to the occurrence of an event, wherein the event is one of group of internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation); and

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20).

However, Serbinis does not explicitly disclose wherein the external events are external to the server computer; nor providing a reference to the process-driven security policy to a client computer, the reference referring to the process-driven security policy state machine and an accessor user list resident on the server computer.

Nonetheless, Troyansky et al. discloses a similar invention and further discloses wherein the external events are external to the server computer(central decision system) [page 19, paragraph 0899]; and nor providing a reference to the process-driven security policy to a client computer, the reference referring to the process-driven security policy state machine and an accessor user list resident on the server computer(allowed recipients information for an *associated document...certain group of individuals can override a specified subset of the security* provisions for a group of documents) [page 3, paragraph 0119 & page 19, paragraph 0897].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Serbinis with the additional features of Troyansky et al., in order to allow for monitoring and controlling of unauthorized dissemination of electronic documents on a portable media and enforcement of a distribution policy associated with the documents, as suggested by Troyansky et al. [page 1, paragraphs 0005-0007].

Regarding **Claim 23**, the rejection of claim 22 is incorporated and Serbinis further discloses wherein the transitioning is performed at the server computer (see, Column 7, lines 63-67).

Regarding **Claim 24**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the associating associates the reference to a group of documents (See, Column 7, lines 22-23 as modified with Leser).

Regarding **Claim 25**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy (See Column 7, lines 54-57, Column 10, lines 59-64 and also Column 3, lines 16-27).

Regarding **Claim 26**, the rejection of claim 21 is incorporated and Serbinis further discloses evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document (see Column 7, lines 63-67).

**Claim 28:** Serbinis discloses a computer program for imposing access restrictions on electronic documents, the program instructions comprising:

Instructions to providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of different states (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and transition rules associated therewith (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and wherein each of the different states has distinct access restrictions for secured documents which reside in that state (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.") and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another (see Column 8, lines 1-20, "Document instances with a "pending" state have an active

date/time that specifies the time at which the state of the document instance should be changed to "active.") and wherein the circumstances include the occurrence of internal and external events (see, Column 7, lines 63- 67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time." And also Column 8, lines 26-29, "Document instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time"). Note: see reply to arguments section for detailed explanation).

transitioning the process-driven security policy from one state to a current state (see, Column 8, lines 1-20).

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20).

However, Serbinis does not explicitly disclose wherein the external events originate from outside the server machine; nor instructions to provide a reference to the process-driven security policy to a client machine, wherein the reference refers to the process-driven security policy state machine and an accessor user list resident on the server machine.

Nonetheless, Troyansky et al. discloses a similar invention and further discloses wherein the external events originate from outside the server machine(central decision system) [page 19, paragraph 0899]; and instructions to provide a reference to the process-driven security policy to a client machine, wherein the reference refers to the process-driven security policy state machine and an accessor user list resident on the server machine(allowed recipients information for an

*associated document*...certain group of individuals can override a specified subset of the security provisions for a group of documents) [page 3, paragraph 0119 & page 19, paragraph 0897].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Serbinis with the additional features of Troyansky et al., in order to allow for monitoring and controlling of unauthorized dissemination of electronic documents on a portable media and enforcement of a distribution policy associated with the documents, as suggested by Troyansky et al. [page 1, paragraphs 0005-0007].

**6. Claims 9 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis et al. (6,584,466) in view of Troyansky et al. (2005/0168766) and further in view of Dutta et al. (6,976,259).**

Regarding **Claim 9**, the rejection of claim 1 is incorporated and Serbinis does not explicitly disclose wherein the external events originate from a second document security system.

Dutta et al. (US 6,976,259 B1) discloses document security system (see, Fig. 2, Numeral 70) in which change to states is triggered by external events which are originated from a second document security system (see, Fig. 2 and also Column 6, lines 17-23).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add, in the system of Serbinis and Troyansky et al., a server which administer state changes for the document security system as taught by Dutta because "In this way, the system is more flexible in that changes made in a central location (e.g. object store 70) are replicated to a plurality of clients." (Dutta, Column 6, lines 21-23).

Regarding **Claim 22**, the rejection of claim 21 is incorporated and the combination of Serbinis and Leser does not explicitly disclose wherein the external events are external to the server computer and the client computer.

However, Dutta discloses wherein external events are external to a document security server and the client computer (see, Fig. 2 and also Column 6, lines 17-23).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add, in the system of Serbinis and Troyansky et al., a server which administer state changes for the document security system as taught by Dutta because "In this way, the system is more flexible in that changes made in a central location (e.g. object store 70) are replicated to a plurality of clients." (Dutta, Column 6, lines 21-23).

**7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis et al. (6,584,466) in view of Troyansky et al. (2005/0168766) and further in view of Li et al. (2004/0193912).**

Regarding **Claim 10**, the rejection of claim 9 is incorporated and Serbinis does not teach that the transition rules are written in XML.

However, Smith et al. in the same field of endeavor of network security discloses writing security policies in XML format (Paragraph 0014, "In one embodiment of the present invention, the security policies are stored in a relational database in a native Extensible Markup Language (XML) format")

Therefor, it would have been obvious at the time the invention was made to one of ordinary skill in the art to write the transition rules of Serbinis and Troyansky et al. in XML format as taught by Li because XML is a text-based and platform independent, as a result policy

server would be able to enforce and distribute the policies to all client having any type of operating system platform.

## Allowable Subject Matter

8. **Claims 12, 19 and 20** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

## Response to Arguments

9. Applicant's arguments, see pages 17-19, filed 07/13/10, with respect to the rejection(s) of claim(s) 1, 14, 21, 27 and 28 under 35 U.S.C. 102 & 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Troyansky et al. (2005/0168766).

As per **MPEP 704.1**, when an examiner is assigned to act on an application which has received one or more actions by another examiner, the second examiner generally should not take an entirely new approach to the application and/or attempt to reorient the point of view of the previous examiner.

Examiner notes that in view of the remarks filed on 07/13/10, the core arguments suggest that the combination of Serbinis and Leser does not disclose providing a "reference" to an external security policy, and in particular appear to be directed to the fact that Leser provides the entire policy itself instead of providing a mere reference to an external policy.

The newly discovered reference, Troyansky et al., clearly discloses the concept of providing a mark that contains only a "reference" to an external distribution policy [page 3, paragraphs 0110-0116], as opposed to providing the entire policy.

Therefore, Examiner respectfully submits that the combination of Serbinis and Troyanskye et al. fully satisfies each and every limitation of the claimed invention.

## Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Edward Zee/
Examiner, Art Unit 2435